

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
17 February 2005 (17.02.2005)

PCT

(10) International Publication Number
WO 2005/015370 A1

(51) International Patent Classification⁷: G06F 1/00,
H04L 29/06

(21) International Application Number:
PCT/IT2003/000505

(22) International Filing Date: 11 August 2003 (11.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): TELE-
COM ITALIA S.P.A. [IT/IT]; Piazza degli Affari, 2,
I-20123 Milano (IT).

(72) Inventor; and

(75) Inventor/Applicant (for US only): ABENI, Paolo [IT/IT];
Telecom Italia S.P.A., Via G. Reiss Romoli, 274, I-10148
Torino (IT).

(74) Agents: MARKOVINA, Paolo et al.; Pirelli & C. S.p.A.,
Viale Sarca, 222, I-20126 Milano (IT).

(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,

CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,
SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

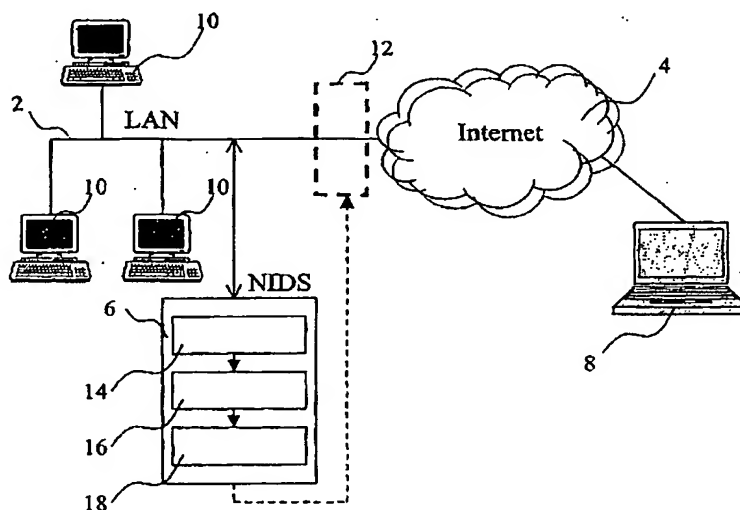
(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,
SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted
a patent (Rule 4.17(ii)) for the following designations AE,
AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA,
CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES,
FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH,
PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN,
TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR DETECTING UNAUTHORISED USE OF A COMMUNICATION NETWORK



(57) Abstract: A system (6) for detecting unauthorised use of a network is provided with a pattern matching engine (16) for search-
ing attack signatures into data packets, and with a response analysis engine (18) for detecting response signatures into data packets
sent back from an attacked network/computer. When a suspect signature has been detected into a packet, the system enters an alarm
status starting a monitoring process on the packets sent back from the potentially attacked network/computer. An alarm is generated
only in case the analysis of the response packets produces as well a positive result. Such intrusion detection system is much less
prone to false positives and misdiagnosis than a conventional pattern matching intrusion detection system.

WO 2005/015370 A1



patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)
 — of inventorship (Rule 4.17(iv)) for US only.

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.